SIMMONS HANLY CONROY, LLC
Jason 'Jay' Barnes (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: (212) 784-6400
Facsimile: (212) 213-5949
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
Nicole Ramirez Jones, State Bar No. 279017
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
koncius@kiesel.law
ramirezjones@kiesel.law

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Joseph P. Guglielmo (admitted *pro hac vice*)
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: (619) 233-4565
Facsimile: (619) 233-0508
jguglielmo@scott-scott.com

Attorneys for Plaintiffs and the Proposed Class
Additional Counsel Listed on Signature Page

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

**LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP**
Michael W. Sobol, State Bar. No. 194857
Melissa Gardner, State Bar No. 289096
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008
msobol@lchb.com
mgardner@lchb.com

**LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP**
Douglas Cuthbertson (admitted *pro hac vice*)
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: (212) 355-9500
Facsimile: (212) 355-9592
dcuthbertson@lchb.com

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

JOHN DOE, *et al.*, individually and on behalf of all others similarly situated,

Plaintiffs,

GOOGLE LLC,

Defendant.

This document applies to: All Actions

Case No. 3:23-cv-02431-VC

PLAINTIFFS' SUPPLEMENTAL RESPONSE IN OPPOSITION TO GOOGLE'S MOTION TO DISMISS FIRST AMENDED COMPLAINT

Judge: Hon. Vince Chhabria

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

INTRODUCTION

Plaintiffs respectfully submit this supplemental brief in response to the Court's Order Requesting Further Briefing, ECF No. 145 ("Order"). The Order asked specific questions about the factual allegations in Plaintiffs' First Amended Complaint ("FAC") as they relate to the privacy, contract, CIPA and ECPA claims alleged. Below, Plaintiffs first address those factual questions in the context of the FAC's allegations, and then turn to the specific claims and why the facts alleged in the FAC support denying Google's motion to dismiss.

ARGUMENT

I. PLAINTIFFS' RESPONSE TO FACTUAL QUESTIONS

The Court's questions relate to a perceived gap between Plaintiffs' factual allegations concerning the operation of Google Source Code, and the inference that Google knows that it is "actually receiving private health information" from Health Care Providers and using that information in Google's "advertising machinery." Order at 1-2. The FAC addresses these issues by alleging: (A) Google provides the same source code to all users, which it calls "publishers" or "developers"; (B) all users are subject to the same terms and policies; (C) Google's willfulness, intent, and knowledge are adequately alleged because (1) Google itself contravenes and does not enforce policies against the transmission of Health Information to Google via Google Source Code, which (2) occurs on 91% of Health Care Provider websites, and (3) benefits Google in its advertising machinery and otherwise. These allegations are as follows:

A. Google Offers All Users the Same Google Source Code.

Google Source Code is the same, and operates identically, for Health Care Providers as it does for other web properties. As alleged, Google Source Code is "provided by Google in a copy-and-paste format" such that its "functionality is uniform on all web properties." FAC ¶ 40; *see also, e.g.,* Ex. 4 at 7 ("To install the tag, copy and paste it into the code").

One universal function of Google Source Code common to all developers is the transmission of individuals' HTTPS Requests (*see* FAC ¶ 51), including: (1) "[i]dentifiers" like

"IP address" and "cookies" (*id.* ¶ 60); (2) the "Request URL" (*id.* ¶ 61); and (3) "Query String Parameters" that contain "additional information" referred to as "field[s]" that have a "corresponding 'value[.]'" *Id.* ¶ 64; *see also id.* ¶ 51 (diagram showing functionality for Google Analytics). In addition, the Google Source Code "deposit[s] the Google Analytics cookies, named _ga, _gid and _gcl_au, on the patient's computing device" and "disguises these cookies as 'first-party' cookies that belong to the Health Care Provider" (*id.* ¶ 54), thus "circumvent[ing] security measures that would prevent third-party tracking via third party cookies." *Id.* ¶ 56; *see also id.* ¶ 449 (*i.e.* places "ghost cookies" on the web visitor's device). Google Source Code also universally "retrieve[s]" data through either "POST" or "GET" requests. *Id.* ¶ 71. These "POST" and "GET" requests are "require[d]," by design, to send the data to "Google . . . domains" as the final endpoint. *Id.* ¶ 70. The specific domains—*e.g.*, "www.Google-Analytics.com" and "analytics.google.com" (*id.* ¶ 47)—are locations associated with Google's advertising machinery. *See id.* ¶ 46 (Analytics is "'[d]esigned to work seamlessly with'. . . other Google marketing and advertising products"); *id.* ¶ 188 ("Google ties the Health Information together and associates all of it together through Join IDs and identifiers that it collects across different services."); *see also* § C-3, *infra*, (discussing other advertising domains).

B. All Users Are Subject to the Same Policies

Google's instructions, descriptions of its products, help pages, and policies are the same for all developers that use Google Source Code, *i.e.*, there are no contracts or policy documents unique to Health Care Providers or any particular industry. *See, e.g.*, FAC Exs. 1-6; 8-29; 41-44; 48-50; 53-55 (uniform support and policy documents); ECF No. 89, Ex. 1 (same). While Google support documents instruct developers not to use its source code in a manner that violates "user privacy" (*e.g.*, "publishers must not pass any data to Google that Google could use or recognize as personally identifiable information (PII)" (FAC Ex. 55 at 1)), Google knows and acknowledges that the information transmitted via Google Source Code "often" violates its written policies. For example, Google acknowledges that "[t]he basic Analytics tag collects the page URL and page title of each page that is viewed. PII is often *inadvertently* sent in these URLs and titles. . . ." *Id.*

¶ 334 (emphasis added). Google suggests that publishers can control the transmission of PII to Google (*see id.* ("you'll need to remove it")), but this is misleading because "the 'basic Analytics tag' is designed to, and does, *automatically* . . .collect PII in the form of the 'cid' data parameter that Google inserts into the page URL, and then connects to user identifiers." *Id*. (emphasis added). Similarly, "[w]hen the Google Source Code for Google Ads is present on a Health Care Provider's web property, the source code deposits an NID Cookie (or accesses an existing NID Cookie) on the patient's computing device," which is associated with Google Account identifiers "such that any future communication by a patient who is not signed into her Google Account can be identified by Google by using the NID cookie to link that patient to her Google Account." *Id*. ¶ 77.

Google also acknowledges on a support page that Google Source Code's default, universal operations will violate HIPAA if used on "HIPAA-covered" web pages like those at issue in this case. Specifically, Google recognizes that using Google Source Code on such web pages would result in the collection of Health Information without adequate consent, and the only way to avoid this is not to use Google Source Code, *e.g.*: "Customers who are subject to HIPAA. . . may only use Google Analytics on pages that are not HIPAA-covered" (*id.* ¶ 410(a)), "[a]uthenticated pages are likely to be HIPAA-covered and customers should not set Google Analytics tags on those pages" (*id.* ¶ 410(b)), and "[u]nauthenticated pages that are related to the provision of health care services . . . are more likely to be HIPAA-covered." *Id.* ¶ 410(c); *see also* FAC Ex. 1 at 1-2 ("Google makes no representations that Google Analytics satisfies HIPAA requirements and does not offer Business Associate Agreements."); FAC ¶ 238 (summarizing the same facts as reflected in in the 2022 HHS Privacy Bulletin).

C. The Facts Alleged Show that Google Willfully Obtains Health Information

But Google's nod to HIPAA on a support page does not mandate (or even support) an inference that Google does not want or intend Health Care Providers to use Google Source Code on HIPAA-covered webpages. Nor does it support an inference that if and when Health Care Providers do use Google Source Code it operates in a unique way. Numerous facts alleged support the contrary inferences, favorable to Plaintiffs, that Google's acknowledgment of these risks is merely intended to provide Google with a modicum of deniability for unlawful activities that it actually encourages and intends.[1]

1. Google Chooses Not to Enforce Its Purported Policies

Plaintiffs allege that, despite its promises and ability to do so, Google takes no action to enforce its policies. Google can identify web properties as belonging to Health Care Providers, including by "using (1) its search index spider to identify health care properties with key terms required by law and (2) content categorizations that Google has publicly stated it has applied to web properties." *Id.* ¶ 206; *see also id.* ¶¶ 207-211 (describing index search that could use terms in mandatory HIPAA notice); *id.* ¶ 219 (describing verticals Google "employs or has employed internally to categorize the content of particular communications and/or web properties"). Google also receives and processes the HTTPS Request data intercepted by Google Source Code (*see* § A, *supra*) and thus knows what the information contains and where it came from (*see* § C-3, *infra*, discussing Google domains). Google claims to "use[] the information shared by sites and apps to . . . protect against fraud and abuse" (*id.* ¶ 288), and that Google will enforce "basic rules of conduct [that require those using Google services to] comply with applicable laws . . . [and] respect the rights of others." *Id.* ¶ 280. But there is no indication that this occurs; beyond issuing general policy statements, "Google takes no further actions to identify and prevent the collection of Health Information from Health Care Providers." *Id.* ¶ 411.

2. Transmission of Health Information to Google is Widespread

Google Source Code is used extensively on Health Care Provider web properties despite the fact that these websites, by their nature, are operated by HIPAA-covered entities, have authenticated pages (behind portals), and have numerous unauthenticated pages that are related to the provision of health care services. *See* § B, *supra*. Plaintiffs confirmed the functionality of

[1] This is true even without allegations that "Google engaged in a plot to deceive providers into disclosing private health information" (Order at 3), which are not required for any of Plaintiffs' claims. Though this is beside the point, as the FAC does contain allegations that Google misled Health Care Providers into believing it will "prevent abuse of its systems" and "will not collect or monetize Health Information." FAC ¶ 306

Google Source Code, and its interception of health information, in an extensive pre-filing forensic review of 5,297 Health Care Provider web properties, which revealed that "Google is unlawfully tracking and acquiring patient Health Information from 91 percent of Health Care Provider properties examined," including 60% for Google Analytics, 59% for Google Ads, and 50% for Google Display Ads. FAC ¶ 155.

Plaintiffs also investigated the information transmitted by specific Health Care Provider web properties, as evidenced by the transmission of data to Google collection endpoints (*id.* ¶ 47 (Google Analytics), ¶ 74 (Google Ads), ¶ 86 (Google Display Ads)) in actual practice, to provide representative examples of the information Google Source Code present on these web properties was configured to—and did—collect. Plaintiffs describe how Google Source Code can transmit identifiable data to Google's servers about the "services, medical appointments, medical conditions, treatments, [and] health insurance" of patients (*id.* ¶ 61), as well as the "doctors, conditions, treatments, services" Plaintiffs received (*id.* ¶ 62). Plaintiffs alleged additional details of their findings concerning Google Source Code on the MedStar and Gundersen websites as illustrations. *See*, *e.g.*, *id.* ¶ 55 ("When a patient visits the MedStar homepage or patient portal, the Google Source Code deposits the Google Analytics cookies on to the patient's device and designates these cookies as belonging to MedStar"). Plaintiffs provided illustrative examples of a URL containing information about a search for providers at Gundersen (Cardiologist Jason R. Darrah), and the URL transmitted when a patient visits their "my chart" portal page. *Id.* ¶¶ 66, 83. Plaintiffs provided even more detail concerning each Plaintiff's experience and the information transmitted in Plaintiff-specific allegations. *See id.* ¶¶ 20-31, *including e.g.*, *id.* ¶ 20 ("Investigation reveals that Google intercepted and shared without authorization at least the following information about Jane Doe I's communications on the MedStar and Mercy MD web properties: communications related to doctor searches specific to her medical needs, including searches . . . communications about payment of bills; communications about her log-ins to the MedStar and Mercy MD patient portals; communications about when she views medical records and lab results within the patient portal; and communications about her specific conditions or treatments").

The forensic testing allegations at this early stage is sufficient, with the other facts alleged, to make plausible Plaintiffs' theory that Google's policies are neither intended, nor effective, to prevent the transmission of Health Information to Google. The allegations above, which indicate that at least 91% of Health Care Provider sites tested redirected data to Google, including on authenticated and treatment-related web pages, supports the inference of Google's uniform functionality and interception of Health Information despite any policies or support documents to the contrary.

3. Google Benefits from Receiving Health Information

Google benefits from Health Care Providers' widespread use of Google Source Code on web pages that contain Health Information. Google "is an established advertising company (*id.* ¶ 34), that "generates revenues primarily by delivering targeted online advertising" (*id.* ¶ 32). As alleged, "Google Analytics, Google Ads, and Google Display Ads" are "advertising products." *Id.* ¶ 124. "A fundamental and primary purpose of Google Analytics is to obtain the information about consumers' communications and activities that is accessible by entities other than Google." *Id.* ¶ 45. Where Google Source Code is present, as it is on the web properties that Plaintiffs used, the data it transmits is routed to domains Google uses for its advertising business, *i.e.* its "advertising machinery": Google Analytics interceptions occur through the domains "www.Google-Analytics.com" and "analytics.google.com." *Id.* ¶ 47. Data intercepted by "Google Ads" and "Google Display Ads" is routed to several known advertising-related domains, such as "adservice.google.com," and "www.doubleclick.net," respectively. *Id.* ¶¶ 74, 86. Google's SDK functions similarly, sending "app event data" from the "mobile app user's device" to specific "Google[] servers" known as endpoints. *Id.* ¶ 102. The data received through Google Source Code is "use[d] . . . within" these specific "products" and thus in Google's advertising machinery. *Id.* ¶¶ 124*; see also id.* ¶ 43 (alleging that these "products" are "designed for the express purpose" of engaging in "hyper-specific targeting of individuals"); *id.* ¶ 117 ("Even when Google does not directly monetize the Health Information, it uses it to learn aggregate information to improve Google's own business . . . improve its search algorithms and other ad-related capabilities . . .

improve its machine learning models . . ."); *id.* ¶ 118 (on data mining, "Google maintains access to real identifiers and the identity of those users in its own databases for its own purposes").

Plaintiffs also make numerous allegations regarding how Google uses data collected via Google Source Code and associates it with other identifiers. *See, e.g.*, *id.* ¶ 77 (associations between NID Cookie and Google Account); *id.* ¶ 127 ("Conversion Tracking"); *id.* ¶ 129 ("attribution models"); *id.* ¶ 143 (remarketing); *id.* ¶ 194 ("signed-out browser identifier cookies"). Google acknowledges that it uses the information it receives via Google Source Code for ads purposes "to target ads based on user interests via 'placements,' 'keywords,' and 'contextual targeting' on Non-Google Websites and Apps" (*id.* ¶ 147) by "match[ing] ads to relevant sites in [Google's] Display [Ads] Network using [] keywords or topics, among other factors" including "language and location targeting, [and] a visitor's recent browsing history." *Id.* ¶ 153.

While the Court questions whether Plaintiffs can prove their allegations that Google uses Plaintiffs' Health Information "for its marketing and advertising purposes" (*id.* ¶ 105) when Plaintiffs have not alleged that they started receiving targeted ads after visiting a Health Care Provider web property with Google Source Code (*see* Order at 2) this is at best one example of a use that could support plausible claims—not the only one. For example, the FAC alleges that data redirected to Google Ads is used for "Conversion Tracking" and "attribution models"—two "essential" features of "Google's advertising business." *Id.* ¶¶ 127, 129. This use case, like other purposes beneficial to Google discussed herein, would not necessarily result in a targeted ad based on the collection of Plaintiffs' and Class members' Health Information—as the Court envisions—but is nonetheless a direct and equally actionable unauthorized use of protected data.

D. Plaintiffs' Theory of the Case Is Facially Plausible

The crucial facts alleged for purposes of unwinding misconceptions about the FAC identified in the Order are that, where the source code is installed—which it is on the large majority of Health Care Provider web properties tested, including "portal" and other HIPAA-covered pages used by the Plaintiffs—it sends HTTPS requests with identifying data, the full contents of URLs including search terms, and information about patients' healthcare, from web property visitors to

Google's advertising domains. The FAC does rely, in part, on "Google's description of how its services work *generally*" (Order at 1) because as discussed above, no facts suggest that the "copy-and-paste format" (FAC ¶ 40) of Google Source Code behaves differently on the estimated "91%" of Health Care Provider web properties tested (*id.* ¶ 1), than it does elsewhere, or that Google prevents itself from using the data, once received, consistent with its general practice (*id.* ¶ 4). Given Google's control of "[a]ll operations relevant to this Complaint" including its role as "the creator of the Google Source Code" (*id.* ¶ 32), Plaintiffs allege that despite Google's claims to the contrary—Google (1) knew from "detailed content categorizations for websites and webpages" which pages "related specifically to Health Information and Health care Providers" (*id.* ¶ 305); (2) chose to nevertheless intercept and receive this data from at least "91%" of Health Care Provider web properties tested through the Google Source Code (*id.* ¶ 1); (3) "encourage[d]" all Health Care Providers to "use the same tools as any other advertiser or publisher" (*id.* ¶ 306); and (4) did "not make use" of any of its "actual systems" to "prevent the collection of Health Information from Health Care Providers" (*id.*).

Plaintiffs individually allege that their protected communications and activities were captured by Google Source Code on Health Care Provider web properties (*id.* ¶¶ 20-31), which is plausible in light of its widespread deployment. Instructive on this point is *Jewel v. National Security Agency*, 673 F.3d 902 (9th Cir. 2011). In *Jewel*, the District Court dismissed privacy claims relating to NSA surveillance because, other than "specific allegations that the NSA used AT&T's Folsom Street facility," the complaint contained "no other allegations specifically linking any of the plaintiffs to the alleged surveillance activities." *Id.* at 907. On appeal, the Ninth Circuit reversed, holding that the allegations were sufficiently particularized when they described defendant's actions as a "network of surveillance," and pled "the technical means," the equipment used, and "that her communications were part of the dragnet." *Id.* at 910. Plaintiffs have done this here: pleading that their Health Care Providers are caught in Google's "network of surveillance", the "technical means" through which the surveillance is accomplished (*i.e.,* the Google Source Code), and that all such acquired data, including Plaintiffs' communications, were fed into part of

Google's system and automatically incorporated into it advertising machinery.

The Court therefore can properly infer from the FAC "that Google is knowingly, willfully or intentionally acquiring private health information and allowing that information be fed into its advertising systems" (Order at 2), which Google uses for its marketing and advertising purposes. *See Smith v. Google, LLC*, No. 23-CV-03527-PCP, 2024 WL 2808270, at *5 (N.D. Cal. Jun. 3, 2024) (interpreting some of the same Google policies and technology and holding that "[w]hile Google argues that judicially noticeable policy documents suggest that Google did not actually want to receive personally identifiable information and expressly prohibited developers from transmitting such data, this presents a question of fact"). As in *Smith*, Google's ostensible policies and support pages, at most, raise questions of fact when compared to its conduct that should be resolved with a full evidentiary record. *See In re Meta Pixel Tax Filing Cases*, No. 22-CV-07557-PCP, 2024 WL 1251350, at *4 (N.D. Cal. Mar. 25, 2024); *see also Doe v. Meta Platforms, Inc.*, No. 22-CV-03580-WHO, 2023 WL 5837443, at *3 (N.D. Cal. Sept. 7, 2023) (even if "Meta may tell third parties. . .that it intends to prevent receipt of sensitive health information," "[w]hat Meta's true intent is" and "what steps it actually took to prevent receipt of health information . . . turn on disputed questions of fact that need development on a full evidentiary record"); *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 684 (N.D. Cal. 2021) (at the pleading stage "interception may be considered intentional 'where a defendant is aware of the defect causing the interception but takes no remedial action'") (quoting *In re Google Asst. Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020)); *U.S. v. Galecki*, 89 F.4th 713, 719 (9th Cir. 2023) (company's "official position" that product was "not for human consumption" did not prove company's lack of intent to sell product for human consumption).

While the Court may be skeptical that Google actually intended the widespread violation of law and policy that it knew or should have known about, permitted, and benefited from, Plaintiffs claims are not "facially implausible" in light of all the facts alleged and should be allowed to proceed to discovery. *See In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1057 (9th Cir. 2008) ("skepticism is best reserved for later stages").

II. PLAINTIFFS' RESPONSE TO QUESTIONS REGARDING SPECIFIC CLAIMS

A. Common Law and Constitutional Invasion of Privacy

As noted in the Order, common law and constitutional privacy claims require the "inva[sion] of a "serious privacy interest" and that the invasion would be "highly offensive to a reasonable person." Order at 3. Given the sensitivity of health data, the "transmit[al]" and "capturing" of this information without consent of the end user (*i.e.*, Plaintiffs and Class members) is—by itself—a highly offensive invasion of privacy. *See Doe v. Regents of Univ. of California*, 672 F. Supp. 3d 813, 820 (N.D. Cal. 2023) (allegation that plaintiffs "[medical] information was transmitted to Meta through the Meta Pixel" sufficient to state common law intrusion claim); *Doe v. FullStory, Inc.*, No. 23-CV-00059-WHO, 2024 WL 188101, at *5 (N.D. Cal. Jan. 17, 2024) ("allegations of surreptitious capturing of healthcare information are sufficient to state" the intrusion upon seclusion claim). Further, as this Court has stated, "[u]nder California law, courts must be reluctant to reach a conclusion at the pleading state about how offensive or serious the privacy intrusion is" because it is "a factual question best left for a jury." *In re Facebook, Inc. Cons. Priv. User Prof. Litig.,* 402 F.Supp.3d 767, 797 (N.D. Cal. 2019).

Here, Plaintiffs plausibly allege Google committed privacy torts in two ways. First, Google "deposit[ed] . . . Google Cookies as 'first-party' cookies belonging to Health Care Providers when, in fact, they are third-party cookies belonging to Google." FAC ¶ 438. Put another way, "Google . . . gain[ed] unauthorized access to [patient] devices via web-bugs and 'ghost cookies'" by "placing the _ga, _gcl_au, NID, IDE, DSID, and . . . Account cookies" on patient "computing devices" through "healthcare providers." *Id.* ¶ 450. Second, through its Source Code, Google systematically collected Health Information about Plaintiffs and Class members each time they communicated with their Health Care Providers through their web properties. *See* § C-2, *supra*. Google did not have Plaintiffs' and Class members' consent to do so. *See* FAC ¶ 10 ("Google's own terms of service and privacy policy assure users of all Google products that it will not collect Health Information without users' consent."); *id.* ¶¶ 20-31 (alleging Google collected Plaintiffs' health data "without [their] knowledge or consent").

The unauthorized placement of the "ghost cookies" on patient devices and Google's unauthorized collection of Health Information discussed in Section I are sufficient on their own (and together) to plead a privacy violation. While Plaintiffs additionally include allegations regarding Google's use of this data, which supports their allegations of intent and egregiousness (*see* FAC ¶ 440) pleading a specific use is not an element of a privacy violation. *See* Restatement (Second) of Torts § 652B, cmt. a. ("The intrusion itself makes the defendant subject to liability, even [without] publication or other use of any kind of … the information outlined").

B. Breach of Express Contract

The Court's Order tentatively proposes dismissing Plaintiffs' contract claim for failure to "adequately allege that Google violated a promise to the plaintiffs not to use their personal health information without consent." Order at 3. But the FAC explains that Google promises in its Privacy Policy under the heading "Why Google Collects Data" that it "does not show" "personalized ads" based on "sensitive categories" such as "health" and that it "require[s] the same from advertisers." FAC ¶ 283. Google repeats this promise in "nested presentation of [its] Terms of Service" that its "Personalized advertising" policy prohibits advertising that pertains to "health." *Id.* ¶ 284. The FAC further alleges that Google broke these promises because, as described above, Google's advertising products—including its attribution models used for ad personalization—use the Health Information intercepted from Plaintiffs and Class members through Google Source Code on Health Care Provider web properties; an assertion which is supported as discussed above in Section I. Plaintiffs adequately allege Google's "use" of their Health Information in violation of this promise.

The contract cause of action should also survive because "use" is just one of the promises Plaintiffs allege Google breached though its conduct. Plaintiffs separately allege that Google represented it would not "*collect* Health Information without individuals' consent" in its "Terms of Service and policy documents." FAC ¶ 267 (emphasis added); *id.* ¶ 268 (explaining under "Categories of information we collect" the Google Privacy Policy identifies "health information" as a "distinct category" that will only be collected "*if you choose to provide it*") (emphasis added). Google broke this promise by collecting Plaintiffs and Class members' health data when they did not "choose to provide it." *See* § C *supra*. Thus, Plaintiffs plausibly allege a breach of this promise based on Google's collection of Health Information, regardless of whether the Court credits their use allegations. In addition, Plaintiffs alleged breach of promises summarized as (1) enforcing "basic rules of conduct," such as requiring advertisers to "comply with applicable laws[,] respect the rights of others, including privacy . . . rights" (*id.* ¶ 280), and maintaining rules about "appropriate conduct that everyone using [Google's] services must follow" (*id* ¶ 276); and (2) that Google "uses the information it obtains from other websites and application to enforce the rules of conduct," including to "protect against fraud and abuse in the use of its services." *Id.* ¶ 288; *see also id.* ¶ 289. Proving breach of these promises does not require evidence of advertising use.

C. California Invasion of Privacy Act

California Penal Code § 631 makes it unlawful to "read[] or attempt[] to read, or to learn the contents or meaning of any message report, or communication … *or* [to] use[], or attempt to use, in any manner, or for any purpose … any information so obtained." By using the disjunctive "or" CIPA authorizes Plaintiffs' claim if Google read or learned the contents *or* if it used the contents in any manner or for any purpose.

Plaintiffs' allegations satisfy each alternative prong of CIPA. As described in the FAC, the purpose of collecting data through the Google Source Code is so Google can (1) as an initial matter, "provide detailed reports on all activity that occurs on a web-property" including "aggregate . . . statistics" to the web property provider (FAC ¶ 118); and (2) use the data for Google Analytics, Google Ads, and Google Display Ads, which are the products that directly receive the data obtained through the Source Code. *See id.* ¶ 47-48 (explaining Google Source Code sends the data to the domains for Google Analytics); *id.* ¶ 74-75 (same for Google Ads); *id.* ¶ 86-87 (same for Google Display Ads). It would be impossible for Google to provide these detailed analytics, or its advertising services (*i.e.*, "use[s]" the data), without first "read[ing]" or "learn[ing]" what it contains. Thus, Plaintiffs plausibly allege a claim for a violation of Section 631.

Separate from the above, Section 632(a) prohibits "eavesdrop[ing] upon or record[ing] the confidential communication" without consent. This provision does not contain any requirement that Google "read" or "use" the information; rather, it is satisfied based on Google's unlawful interception or private communications alone. *See Brown v. Google LLC*, 685 F. Supp. 3d 909, 938 (N.D. Cal. 2023) ("Section 632 protects against 'intentional, nonconsensual recording' of communications 'regardless of the content of the conversation' involved or *how parties choose to disseminate it thereafter*") (emphasis added).

D. Electronic Communications Privacy Act

The Order tentatively proposes dismissal of Plaintiffs' ECPA claims on the grounds that the alleged interception was "with the consent of the health providers" and "[P]laintiffs have not plausibly alleged that Google fraudulently induced the providers' consent." Order at 3. As explained below, this claim is also sufficiently alleged.

First, Plaintiffs allege that Google's interception of Plaintiffs' Health Information was without consent—from either Health Care Providers or Plaintiffs and Class members—because Google expressly represented in "Terms of Service and policy documents" (FAC ¶ 267) that it would not collect "health information" unless the individuals personally "*choose to provide it*" to Google. *Id.* ¶ 268 (explaining under "Categories of information we collect" the Google Privacy Policy identifies "health information" as a "distinct category" that will only be collected "if you choose to provide it"). No reasonable Health Care Provider would understand that Google collects consumers' Health Information merely because their webpages incorporate Google Source Code. *Cf. In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 604 n.7 (9th Cir. 2020) ("[I]ndividuals maintain the expectation that entities will not be able to collect such broad swaths of personal information absent consent[]"). Moreover, "[c]onsent to interception can[not] be inferred from the mere purchase of a service, regardless of circumstances." *In re Pharmatrak, Inc.*, 329 F.3d 9, 20 (1st Cir. 2003). Instead, "California law requires the Court to pretend that users actually read [Google's] contractual language before clicking their acceptance" and the Court must assess the contractual language to determine whether someone "agreed" to the conduct at issue. *In re Facebook, Inc., Cons. Priv. User Prof. Litig.*, 402 F.Supp.3d at 789. Nothing in Google's purported contract (ECF No. 89, Ex. 1) or other document before the Court suggests that Health

Care Providers consent to provide protected health information to Google. One would expect to see such an important contractual term front and center if it exists. "If the contract language at issue is reasonably susceptible to more than one interpretation, with one of those interpretations suggesting consent and another belying it, the Court cannot decide the consent issue in [Google's] favor at the motion to dismiss phase." *Id.* That rule is true for developers as well as patients.

The recent decision in *Smith v. Google*, involving some of the same contracts that Google has with developers that are at-issue here, is on point (with the difference being that they were tax software providers instead of healthcare providers):

> With respect to consent, Google argues that because the tax sites 'chose to use Google Analytics, they obviously consented to it.' But this argument draws a crucial inference in Google's favor—that in addition to installing Google Analytics, website operators understood how the software works and what data would be sent to Google and fully consented to that transmission. The complaint alleges that Google purportedly prohibited sending personal information via Google Analytics but nevertheless allowed such information to be transmitted (to its benefit). Taking this as true, the Court cannot presume that every website owner who installed Google Analytics understood exactly what data would be sent to Google and how Google might use it. Whether developers consented to data collection by using Google Analytics is a fact dispute that cannot be resolved at this stage.

Smith, 2024 WL 2808270 at *7, 12. Here, too, Google has not pointed to any contract language that would create consent for the specific conduct at issue in this case.

On the contrary, Health Care Providers' contracts expressly incorporate the Google Privacy Policy in which Google says it only "collects" "Health Information that you choose to provide to it." FAC ¶ 309 (Privacy Policy expressly incorporated into publisher and advertiser accounts for at-issue products). Similarly, for Google Signals (a feature through which Google connects Analytics, Ads, and Display Ads data), Google wrongly promises publishers that "Google is (1) only collecting information where it has a person's consent to do so; (2) not associating signed-in and signed-out activity; and (3) not collecting personally identifiable information through Google Source Code." *Id.* ¶ 314; *see also id.* ¶¶ 315-329 (not quoted due to length, identifying where specific "signals" statements can be found, how they are presented, and why they are not true.) Further, as discussed in Section C above, even Google's support pages purporting to restrict the transmission of PII give "the impression that Google Analytics does not collect personally identifiable information" (*id.* ¶ 330) by failing to warn that "the basic Analytics tag is designed to, and does, automatically collect PII . . . ." *Id.* ¶¶ 330-334.

Second, it is Google's burden to prove consent and, absent some clear evidence that Health Care Providers actually consented to the collection of Health Information (which Google has not provided), Plaintiffs' ECPA claim should not be dismissed on those (or any) grounds.

Third, even if there were consent from Health Care Providers, Google remains liable under the ECPA because the interception was "for the purpose of committing any criminal or tortious act." 8 U.S.C. § 2511(2)(d). Put simply, even if a Health Care Provider could have consented to sharing personally identifiable health information by installing Google Source Code, or otherwise, Google still knew the interceptions would violate HIPAA and the FTC Act and would be otherwise tortious. *See* FAC ¶ 408(b)-(c) (establishing criminal offense for the "knowingly …. obtaining individually identifiable health information relating to an individual" with enhanced penalties when done "with the intent … to use individually identifiable health information for commercial advantage") (citing 42 U.S.C. § 1320d-6); *id.* ¶¶ 240-243 (FTC Act).

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court reconsider its tentative decision to dismiss the FAC in its entirety. Should the Court remain unpersuaded, Plaintiffs respectfully request leave to amend as contemplated by the Court in the Order.

Dated: June 7, 2024

SIMMONS HANLY CONROY LLC

/s/ Jason Barnes
Jason 'Jay' Barnes (admitted *pro hac vice*)
jaybarnes@simmonsfirm.com
An Truong (admitted *pro hac vice*)
atruong@simmonsfirm.com
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: 212-784-6400
Fax: 212-213-5949

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
clevis@lowey.com
Amanda Fiorilla (admitted *pro hac vice*)
afiorilla@lowey.com
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law
Mahnam Ghorbani, State Bar No. 345360
ghorbani@kiesel.law
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel.: 310-854-4444
Fax: 310-854-0812

LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP
Michael W. Sobol, State Bar No. 194857
msobol@lchb.com
Melissa Gardner, State Bar No. 289096
mgardner@lchb.com
Jallé H. Dafa, State Bar No. 290637
jdafa@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel.: 415 956-1000
Fax: 415-956-1008

Douglas Cuthbertson (admitted *pro hac vice*)
dcuthbertson@lchb.com
250 Hudson Street, 8th Floor
New York, NY 10013
Tel.: 212 355-9500
Fax: 212-355-9592

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Hal D. Cunningham, State Bar No. 243048
hcunningham@scott-scott.com
Sean Russell, State Bar No. 308962
srussell@scott-scott.com
600 W. Broadway, Suite 3300
San Diego, CA 92101
Tel.: (619) 233-4565
Fax: (619) 233-0508

Joseph P. Guglielmo (admitted *pro hac vice*)
jguglielmo@scott-scott.com
Ethan Binder (admitted *pro hac vice*)
ebinder@scott-scott.com
230 Park Ave., 17th Floor
New York, NY 10169
Tel.: (212) 223-6444
Fax: (212) 223-6334

Attorneys for Plaintiffs and the Proposed Class